Intro

I'm doing some research into Near Field Communication on mobile devices. I have a USRP N210 and GNU Radio set up on Ubuntu. I want to be able to read and write NFC radio traffic so I can do "card emulation", that is, act like I'm an NFC card.

Basics

The most useful text I've found is "Securing Near Field Communication" by Henning Siitonen Kortvedt which states that NFC operates in the 13.56MHz band and the channel bandwidth is around 1MHz. This document can be found at (http://ntnu.diva-portal.org/smash/get/diva2:347744/FULLTEXT01) Wikipedia says "It operates within the globally available and unlicensed radio frequency ISM of 13.56 MHz. Most of the RF energy is concentrated in the allowed ±7 kHz bandwidth range, but the full spectral envelope may be as wide as 1.8 MHz when using ASK modulation."

The only variable needed to get a uhd usrp started is sample rate. The Nyquist sampling theorem says you can completely reconstruct any signal if the sampling rate is at least 2 * B where B is the highest frequency of the signal. Our signal is at 13.56 Mhz, or 13.56e6 Hz. However, if we center our signal at this frequency (another variable you can pass to the uhd usrp), then the highest frequency of the signal becomes just the channel window / 2. Eyeballing it, or using the Wikipedia estimate, it looks like the channel width is less that 40kHz. That means we need a sample rate of at least 20,000 Hz = 20kHz. However, the smallest sampling rate that the USRP (apparently) supports is around 200kHz. So, we can just go with that and know we'll have more than enough data. Later we can decimate further in software, just making sure we are still seeing 20kHz sample rate.

Next we need to worry about getting a channel filter. This might not even be necessary since we are centered on our frequency and with our sample rate we should be getting rid of anything that is spectrally very large. Two easy options are to just decimate or to decimate and low pass filter. I end up doing both but it doesn't change things much.

Demodulation - theory

Next is modulation. There is information on this in Securing Near Field Communication in Section 2.2.3. There are two different types of NFC devices (Type A and Type B). Depending on which type is in use, there are two possible modulations. I don't know which type devices I have.

Type A (at 106kbps), uses 100% ASK with bit duration (bd) = 128/f_c ~ 9.43e-6 seconds. Responses will be load modulation generating a subcarrier with frequency f_s = f_c / 16 (=847.5 KHz). Section 3.4.3 shows some signals captured in Securing Near Field Communication. An example of a single bit is:

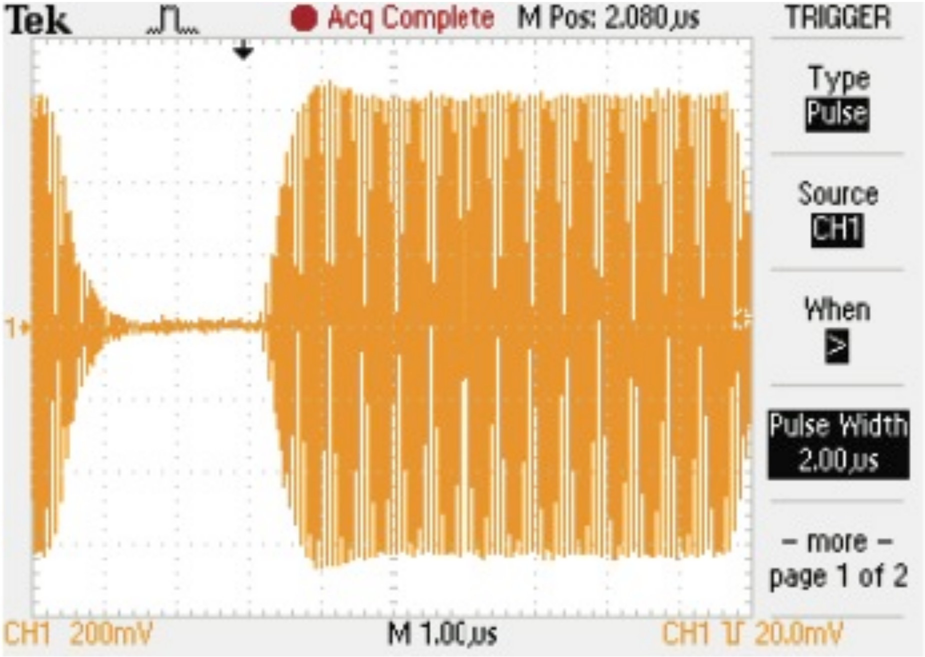


Figure 1: An example 100% ASK encoded bit from the paper.

At higher bit rates, such as 212kbps or 424kbps (f_c/64 or 32 resp), 10% ASK is used. Byte encoding is MSB with Manchester Coding and obverse amplitude. See figure 3.

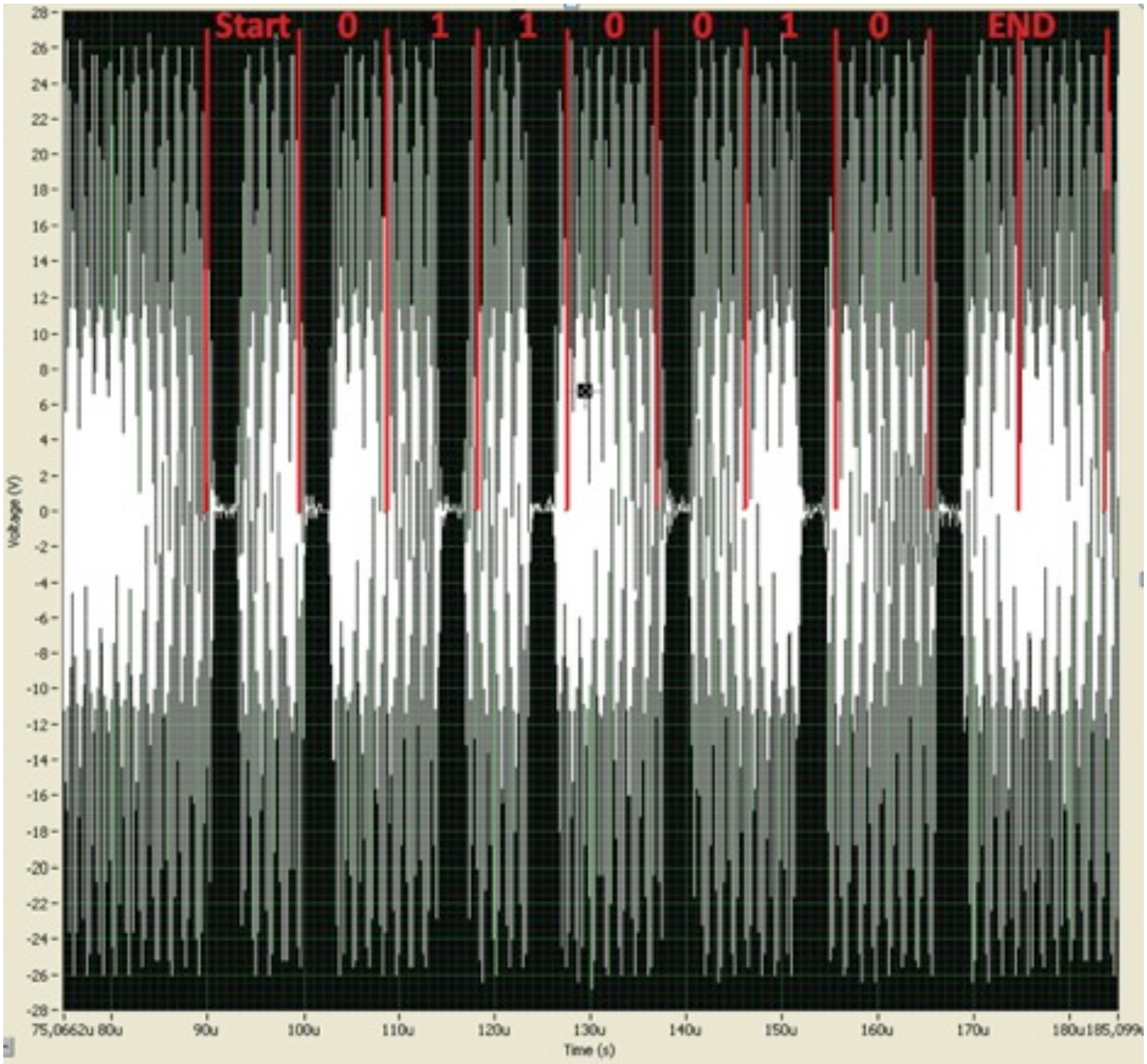


Figure 2: A 100% ASK encoded version of the byte “52” from the paper.

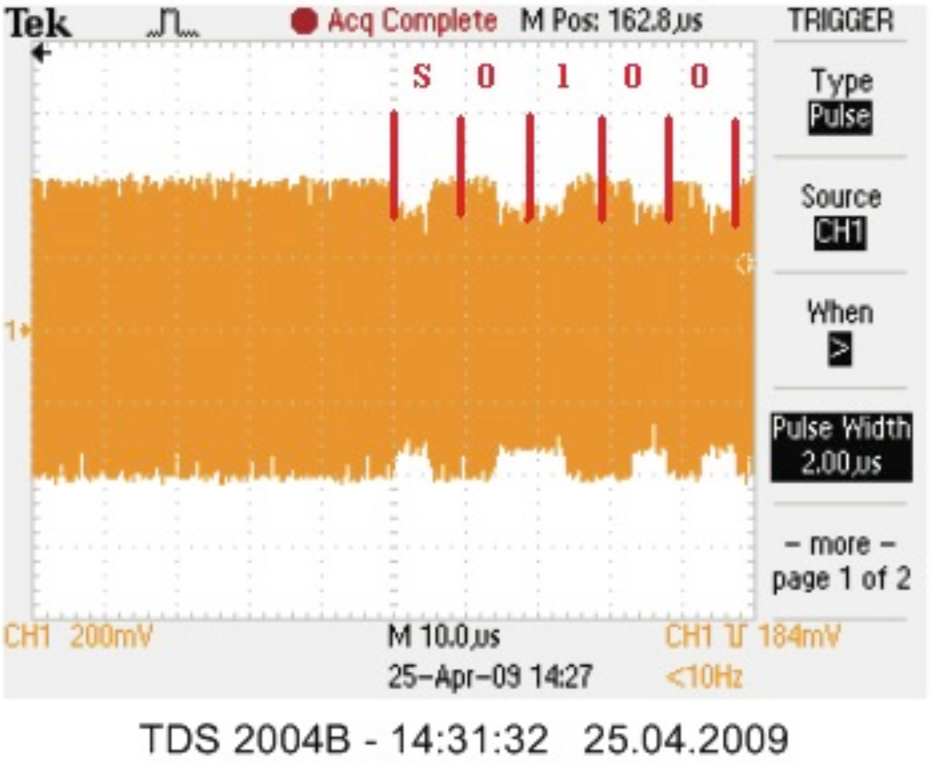
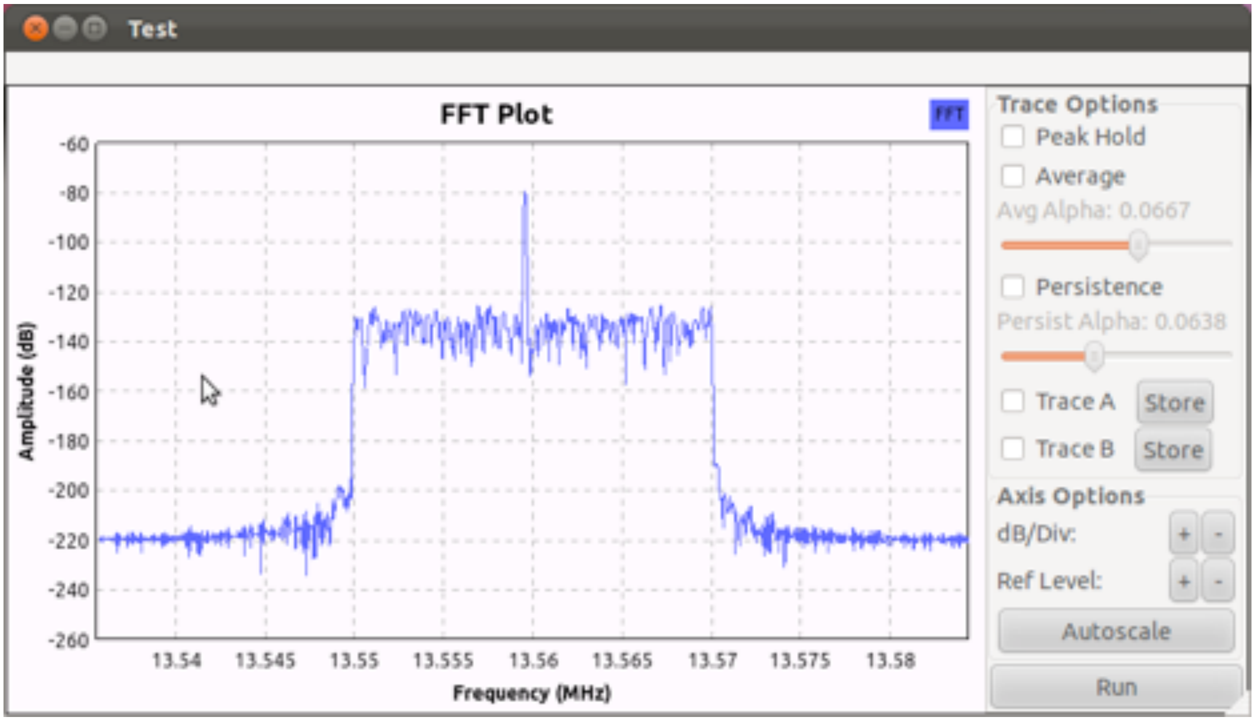


Figure 3: 10% ASK from the paper.

Demodulation - real life

I can capture data and it is around the right frequency. See Figure 4.



□ Peak Hold

□ Average

Avg Alpha: 0.0667

□ Persistence

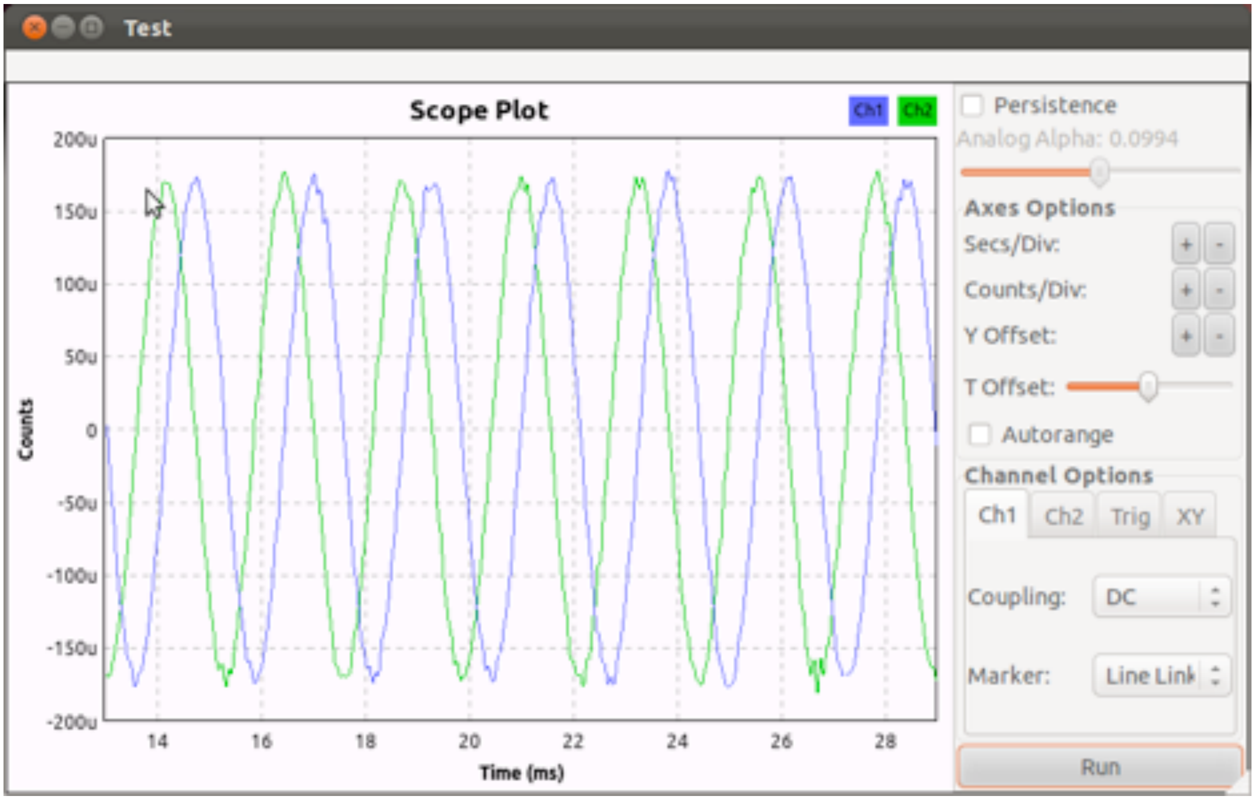
Persist Alpha: 0.0638

□ Trace A

□ Trace B

Figure 4: NFC traffic captured at 195k Samples/Second, decimated by 4, with low pass filter at 10k.

That looks like what I'd expect. However, if I look at the scope output, it is not exactly what I expected, see Figure 5.



□ Persistence

Analog Alpha: 0.0994

□ Autorange

Coupling: DC

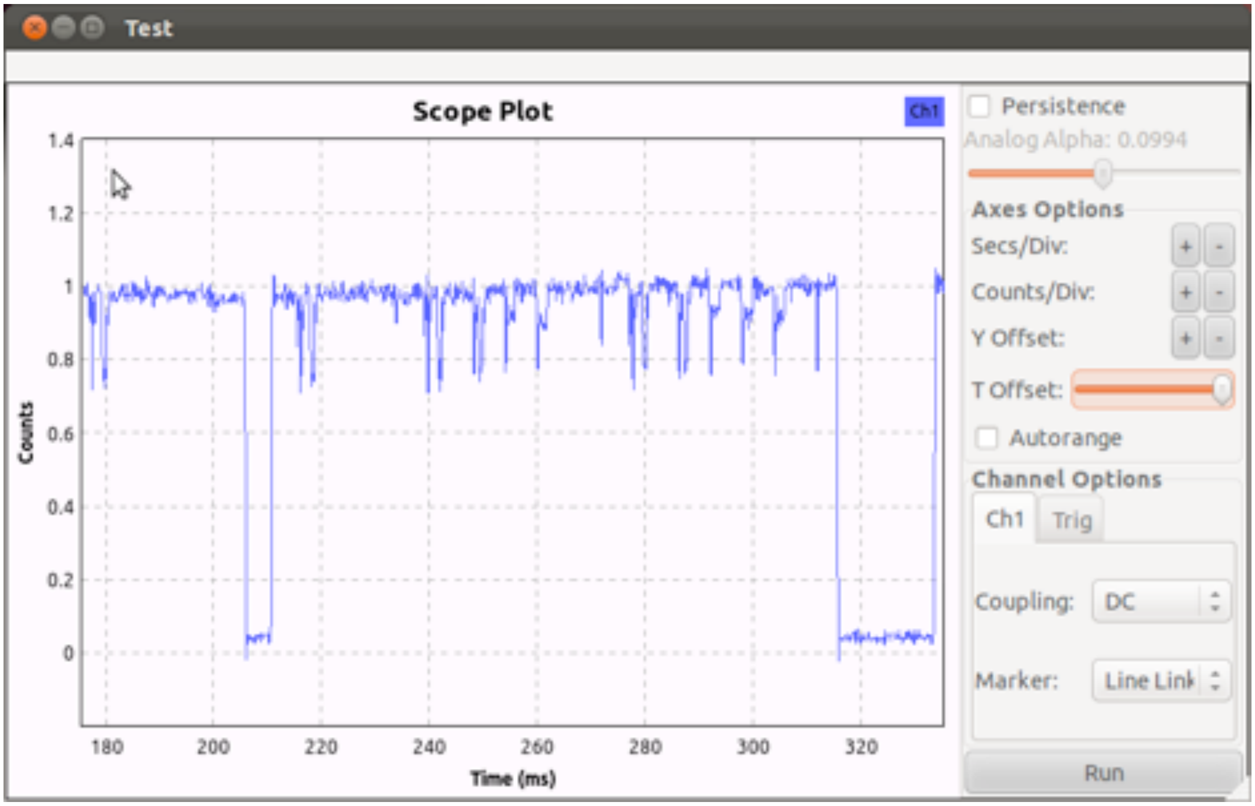
Marker: Line Link

Figure 5: The scope of the NFC signal.

So in Figure 5, it looks like the period of one of the waves is around 2 ms (.002 s) which makes the frequency around 500Hz. You'd expect a period of around 737 micro seconds for a 13.56Mhz signal.

I think the reason I am only seeing a wave with frequency of 500Hz is that I centered my USRP at 13.56MHz. Therefore, really this is a wave of 13.56MHz +/- 500 Hz which is reasonable if you look back at Figure 4. That is, the spectral spike isn't exactly at 13.56MHz.

Anyway, if I blindly try to demodulate the signal, ignoring the above outstanding question, I can graph the magnitude of the signal and look for the ASK (either 10% or 100%). I have no idea if this is the data or noise or what scale I'm looking at, but I see stuff like Figure 6.



□ Persistence

Analog Alpha: 0.0994

□ Autorange

Coupling: DC

Marker: Line Lin

Figure 6. Possible data. I've rescaled it to fit between 0 and 1.

My guess is when the power drops to 0, it is when the field is off. When it is at one, it is on. When it drops down to about .8, it is a 10% ASK pulse. This is just a guess. (Note I rescalled the Y access so that the data was between 0 and 1) The pulses don't look like I'd expect, i.e. they don't look like Figure 3.

Questions

So my signal doesn't look like what I expect. My guess is its got something to do with centering on 13.56mHz so that my signal then looks like 500Hz and 500Hz isn't enough "resolution" to distinguish the data.

I thought maybe I should center at 0 and then get the real 13.56MHz signal but then I need a sample rate of >26M sample/sec and I don't seem to get get data when I try that, presumably it is too fast for my setup but I could be wrong.

Maybe I need to be doing something more complex than taking the magnitude of the signal for generating Figure 6.

Any help would be appreciated! I'm willing to provide more info on my setup, scripts I'm using, data I've captured, etc, just let me know what would be useful.

Refs

http://ntnu.diva-portal.org/smash/get/diva2:347744/FULLTEXT01
http://www.sec.in.tum.de/assets/studentwork/finished/Weiss2010.pdf
http://www.waazaa.org/download/fcd-14443-1.pdf
http://www.waazaa.org/download/fcd-14443-2.pdf
http://www.waazaa.org/download/fcd-14443-3.pdf
http://www.waazaa.org/download/fcd-14443-4.pdf